12-27-99.

A

FORM PTO-1082

Box Patent Application
ASSISTANT COMMISSIONER FOR PATENTS
Washington D.C., 20231

Case Docket No.: 81674-264191
Date: December 22, 1999
Express Mail Label No.: EL331914528US

Dear Sir:

Transmitted herewith for filing is the patent application of
Inventor(s): Anil Vasudevan, Baiju Patel, Marc Jalfon
For: SYSTEM AND METHOD FOR PROVIDING SECURITY MECHANISMS FOR SECURING NETWORK COMMUNICATION

Enclosed are:

X 5 Sheets(s) of drawings (_____ informal)
_____ An assignment of the invention to _____.
_____ An associate power of attorney
_____ A verified statement to establish small entity status under 37 CFR1.9 and 1.27.
X Unsigned Declaration.
_____ Certified copy of Patent Application No. filed from which priority is claimed under 35 U.S.C. §110.
_____ IDS enclosed. _____ with references.
_____ Preliminary Amendment.

CALCULATION OF FEES

	ITEM	NO. OF CLAIMS FILED MINUS BASE*	NO. OF CLAIMS OVER BASE	X SM/LG ENTITY FEE	$ AMOUNT	FEE
A	TOTAL CLAIMS FEE	27 -20*=	7	x $9 or x $18	$ 126	
B	INDEPENDENT CLAIMS FEE**	3 - 3*=	0	x$39 or x 78	$0	
C	SUBTOTAL – ADDITIONAL CLAIMS FEE (ADD FINAL COLUMN IN LINES A + B)					$126
D	MULTIPLE-DEPENDENT CLAIMS FEE			SMALL ENTITY FEE = $130 LARGE ENTITY FEE = $260		$
E	BASIC FEE*			SMALL ENTITY FEE = $380 LARGE ENTITY FEE = $760		$760
F	TOTAL FILING FEE (ADD TOTALS FOR LINES C, D, AND E)					$886
G	ASSIGNMENT RECORDING FEE				$40	$
	**LIST INDEPENDENT CLAIMS 1, 12, 20					

_____ Please charge my Deposit Account No. _____ the amount of $_____ **A copy of this sheet is enclosed.**

_____ A check in the amount of $_____ to cover the filing fee is enclosed.

_____ A check in the amount of $_____ to cover Assignment Recordation fee is enclosed.

____ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. **A copy of this sheet is enclosed.**

__ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.

__ Any patent application processing fees under 37 CFR 1.17.

____ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. .

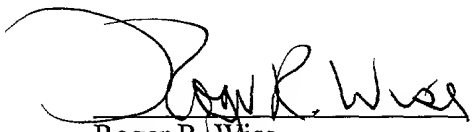
__ Any patent application processing fees under 37 CFR 1.17.

__ The issue fee set in 37 CFR 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(b).

__ Any filing fees under 37 CFR 1.16 for presentation of extra claims.

Respectfully submitted,

Dated: December 22, 1999



Roger R. Wise
Reg. No. 31,204

PILLSBURY MADISON & SUTRO LLP
Intellectual Property Group
Ninth Floor, East Tower
1100 New York Avenue, N.W.
Washington, D.C. 20005-3915
Telephone: (213) 488-7100
Facsimile: (213) 629-1033

PATENT
81674-264191

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Anil Vasudevan, Baiju Patel, Marc Jalfon	Group No.: Unknown
Serial No.: Unknown	Examiner: Unknown
Filed: December 22, 1999	
For: SYSTEM AND METHOD FOR PROVIDING SECURITY MECHANISMS FOR SECURING NETWORK COMMUNICATION	

CERTIFICATE OF MAILING VIA U.S. EXPRESS MAIL
"Express Mail" Mailing Label No. EL331914528US
Date of Deposit: December 22, 1999

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

I hereby certify that

X Letter of transmittal
X Patent application (17 pages of specification; 27 claims; 1 pages of abstract)
X 5 sheet(s) of formal drawings
X Unsigned Declaration
X Return postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service with sufficient postage under 37 CFR 1.10 on the date indicated above and are addressed to:

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231.

December 22, 1999
Date of Deposit

Paula Dunn
Name of person mailing papers

Signature

APPLICATION FOR
UNITED STATES PATENT
IN THE NAME OF

Anil Vasudevan
And
Baiju Patel
And
Marc Jalfon

for

SYSTEM AND METHOD FOR PROVIDING SECURITY MECHANISMS FOR SECURING NETWORK COMMUNICATION

prepared by:
PILLSBURY MADISON & SUTRO LLP
1100 New York Avenue, N.W.
Ninth Floor, East Tower
Washington, D.C. 20005-7100
(213) 488-7100
Attorney Docket No. 81674-264191

Express Mail No.: EL331914528US

SYSTEM AND METHOD FOR PROVIDING SECURITY MECHANISMS FOR SECURING NETWORK COMMUNICATION

BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to computer networks and network security, and in particular, to systems and methods for providing security mechanisms for securing manageability in a computer network.

2. Related Art:

Computer networks in business enterprises, such as a local area network (LAN), wide area network (WAN) or other Ethernet-based systems facilitate communication among computer workstations. With the recent evolution of networking and Internet communications, computer networks have become more open to the world. While this certainly speeds business operations, it brings with it other perils. Having computer networks more open to the world can often leave data and networks traffic open to unintended access. An outsider may install and use a program to monitor the network traffic, alter or modify data streams in transit, or steal an identity to gain unauthorized access into a network. Therefore, a secure environment requires protection at the network level.

A typical LAN couples together one, or a relatively small number of, server systems and potentially large number of client systems. Network traffic communicated between any two systems is in the form of data packets and utilizes protocols regulating the way the data packets are transmitted between the two systems. Many security protocols are provided for securing network traffic. In the case of a LAN, Internet

Protocol Security (IPSec) technology has emerged as the LAN security protocol of choice. IPSec allows business enterprises to add internal LAN protection, building communications security into the data packet itself and securing client/server communications. IPSec operates at the network layer of the protocol stack, i.e., Layer 3 in the Open System Interconnection (OSI) model, and can be used to provide three different types of protection: authentication, integrity and encryption.

IPSec may be applied in many instances. For example, the server system may be a remote management station wishing to communicate certain management traffic to a client system. The remote management station would utilize a management IP based protocol, such as IPSec, to initiate certain management operations on the client system. This is especially true when the client system becomes non-operational, e.g., when the client system is in a pre-boot state, a hung state, or a reset state. In this case, the remote management station would want to send out management commands to try and get the client system back to an operational state. For example, the management commands may include reset, reboot, power down, or power up. These heavy-duty control commands, which can reset or reboot any client systems connected in a network, need to be securely communicated. When a client system is non-operational and another system is trying to manage the client system, care must be taken to make sure that the other system is indeed a management station that the client system trusts.

A typical communication security protocol between two systems has two phases. In the first phase, typically referred to by the name "key exchange", the systems authenticate each other as well as negotiate and agree upon exact parameters and keys to be used to secure subsequent network traffic. The parameters and keys to be

used represent the results obtained after carrying out the key exchange processes, and are often referred to as security association (SA). The SA contains settings like policies and the extent of the strength of the security that is employed on a connection basis. In the second phase, network traffic is secured based on the results obtained in the first phase.

The typical security protocols like the key exchange processes are fairly complex and require many exchanges and computationally intensive operations. This means they do not work well when the operating system (OS) of the client system is absent, i.e., when the client system is non-operational. Although existing security mechanisms, such as those utilizing IPSec and Internet Key Exchange (IKE), are able to secure network traffic when both the client system and server system are operational, they cannot secure network traffic when the OS of the client system is non-operational or absent. There is a need for a method to securely communicate network traffic, regardless of the state of the client system under consideration.

SUMMARY

Embodiments of the present invention are directed to addressing the aforementioned drawbacks associated with providing security mechanisms for securing traffic communicated from one system to another system, even when one of the systems is non-operational. An embodiment of the present invention is directed to a system and method of providing security mechanisms for securing traffic communication between a server system and a client system regardless of the state of the client system under consideration. First, the client system is polled to determine whether it is in an operational state. As soon as the client system enters the operational state, key exchange processes are initiated and executed between the server system and the client system. At the end of the key exchange processes, the results of the key exchange processes are stored into the client system. The traffic communication between the server system and the client system is secured based on the stored results in the client system. In order to maintain a highly secured environment, the stored results in the client system are periodically refreshed and updated with newly obtained results by executing a second set of key exchange processes between the server system and the client system.

However, by inhibiting the stored results in the client system from being updated until a successful execution of the second set of key exchange processes is actually carried out, the system ensures that the traffic is securely communicated even if the client system becomes non-operational. In this case, the system will use the previously negotiated results stored in the client system as the basis for securing the traffic

communication. Thus, traffic communication between the server system and the client system can be secured at all times, even in a non-operation state.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 shows a local area network coupling a server system and a client system according to an embodiment of the invention.

Figure 2 shows in more detail an embodiment of the client system according to the embodiment of Figure 1.

Figure 3 illustrates processes for carrying out security mechanisms according to an embodiment of the invention.

Figure 4 illustrates processes for updating the results of key exchange processes at a server system according to an embodiment of the invention.

Figure 5 illustrates processes for updating the results of key exchange processes at a client system according to an embodiment of the invention.

Figure 6 shows a table illustrating the relationship between a server system and a client system during different state transitions according to an embodiment of the invention.

DETAILED DESCRIPTION

Embodiments of the present invention are directed to a system and method of providing security mechanisms for securing traffic communicated from one system to another system independently of whether the latter system is running normally, or is in a non-operational state. The systems are preferably a server system and a client system, each system containing an operating system and being connected through a computer network. The server system preferably determines whether the client system has entered fully operational state. Once the client system enters the fully operational state, key exchange processes are initiated between the two systems to obtain security parameters for use in securing traffic communication between the two systems. The security parameters, called SA, are the results acquired at the end of the key exchange processes. After the key exchange processes are over, the SA is stored in the client system. To maintain a highly secured environment, the server system periodically refreshes the SA by periodically executing another set of key exchange processes, and communicates the newly obtained SA to the client system for storing them in the client system in place of the original security association. However, the SA is inhibited from being updated in the client system until the server system is successful in completely executing another set of key exchange processes. The traffic communication is then secured based on whichever SA is stored in the client system. Depending on whether the other set of key exchange process is successful, the traffic communication is secured on the basis of either the original SA or the newly obtained SA.

Figure 1 shows a server system 2 and a plurality of client systems 3 coupled in a LAN 1 according to an embodiment of the invention. The typical arrangement of an

environment on a network includes one, or a relative small number of, the server system 2 and a potentially large number of client systems 3. In other embodiments, the server system and client systems may be coupled through a WAN, the Internet, or any other network having an Internet Protocol (IP) based protocol for transmitting data packets.

Figure 2 shows in more detail an embodiment of the client system 3 in Figure 1. The client system 3 includes a network device 4 and a processor 5 for executing computer instructions. According to an embodiment, the processor 5 of the client system 3 includes a central processing unit (CPU) and random access memory (RAM) which is sufficient to support a Windows '95, Windows '98, Windows 2000, or Windows NT 4.0 operating system and application programs compatible with these operating systems. In other embodiments, combinations of different operating systems and different application programs may be implemented in the client system 3. According to an embodiment, a remote server system 2 manages the client system 3 by communicating to client system 3 the management functions required to be performed. In the embodiment, the server system utilizes a management IP based protocol in carrying out certain control/diagnostic operations on a client system 3. In the embodiment, security mechanisms, independent of the state the client system 3 is in, are provided, so that management IP based protocol packets can be securely communicated from the remote server system 2 to the client system 3 at all times. This way, the security mechanisms ensure that the management IP based protocol packets originate from a trusted server system 2. For example, the security mechanisms may be used to secure remote management and control protocol (RMCP) packets using

IPSec through the various stages in the life cycle of the server system 2 and the client system 3.

According to an embodiment, the control/diagnostic operations are performed through the network device 4 in the client system 3. The management IP based protocol is usually fairly simple and uses a particular user datagram protocol (UDP) port to communicate the management traffic. With the security mechanisms, the remote server system 2 securely communicates the management traffic to the network device 4. After the network device 4 intercepts the management traffic, it triggers certain control/diagnostic operations, such as reboot, on the client system 3. In other embodiments, the network device 4 may be considered as the client system, in which the security mechanisms are provided to secure communication between a server system and a network device.

In a preferred embodiment, the security mechanisms operate mainly at the network layer of the seven-layer protocol stack, i.e., Layer 3 in the OSI stack. The network layer embodiment is preferred because of the existence of the IPSec. In other embodiments, the IP based protocol used by the security mechanisms along with the IP based protocol packets may use higher layers of the OSI stack. Moreover, the security mechanisms may be implemented in the data-link layer, i.e., Layer 2 in the OSI stack. For example, the server system may dial in to the client system, and send traffic communication at the point to point protocol (PPP) layer.

Figure 3 illustrates processes for carrying out security mechanisms according to an embodiment of the invention. In step 10, security mechanisms are initiated by a server system to detect whether a client system is operational. If the client system is

operational, key exchange processes are executed between the server system and the client system in step 11, at the end of which the results of the key exchange process, or SA, are obtained. According to one embodiment, key exchange processes are carried out utilizing IKE, which supports the verification of identities. IKE is a hybrid protocol, and its purpose is to negotiate and provide authenticated keying material for IPSec SAs that are used for Authentication Header (AH) and Encapsulating Security Payload (ESP) processing. After the SA is obtained after the execution of the key exchange processes in step 11, the SA is stored in the client system in step 12. In one embodiment, the SA is stored in a network device that is part of the client system. For example, the SA is stored in an Ethernet device. In other embodiments, the network device itself is considered as the client system, and the SA is stored in a component part of the network device. For example, the SA is stored in a coprocessor connected to an Ethernet device or an EEPROM/flash that is part of an Ethernet device.

After the SA is stored, the server system initiates refreshing of the SA by executing another set of key exchange processes based on a SA refresh timer. Periodically refreshing of the SA to generate new SA is required to provide an environment with more security and protection. Steps 13 and 14 may be viewed as mechanisms for inhibiting the SA in the client system from being updated until there is a successful completion of the SA refresh in the server system. The SA in the client system is updated only after a successful refresh is completed. In step 15, the traffic communication is secured based on the results stored in the client system. Thus, depending on whether another set of key exchange processes between the server

system and the client system is successful, the traffic communication is secured either with the SA stored in step 12 or the updated SA in step 14.

According to one embodiment, when the network device in the client system receives a secured packet through the network, it processes the packet to validate security of the packet based on whatever SA is stored in the client system. This may involve, for example, crypotographic hash, decryption, and other processes such as checks for replay attacks. After successful processing of packet for security, the network device forwards the packet to a processor in the client system, allowing normal remote management processing. Similarly, any response generated by the management module to be sent to the server system is also processed for security based on the prior SA negotiation.

Figure 4 illustrates processes for updating SA at a server system according to an embodiment of the invention. In step 20, the server system determines whether the client system is operational. If the client system is non-operational, previously negotiated SA, which is the same SA as the one stored in the client system, is used to secure traffic communication until the client becomes operational. If the client system is operational, the server system determines whether SA should be refreshed based on a SA refresh timer, according to an embodiment of the invention. In step 21, the server system asks whether the SA refresh timer has timed out. If it has not, the previously negotiated SA is used to secure traffic communication until the SA refresh timer has timed out. On the other hand, if the timer has timed out, the server system initiates a SA refresh in step 22 by carrying out another set of key exchange processes. According to an embodiment, the time between consecutive refresh of SA is set to be

significantly smaller than the lifetime of the SA, where the difference must be at least as large as the maximum allowed down time before the client system is managed. In a conservative design, one may choose a very large lifetime for SA, while refreshing SA fairly frequently. For example, the lifetime for SA may be in years, while refreshing the SA may be in hours or minutes.

In step 23, the server system determines whether it has received a "SA is ready for use" signal from the client system. If such signal is not received, the previously negotiated SA is used to secure traffic communication in step 30. If such signal has been received, the server system checks whether the other set of key exchange is successfully completed in step 24. If there is an unsuccessful completion of the SA refresh, the previously negotiated SA is used to secure traffic communication in step 30. If there is a successful completion of the SA refresh, the server system sends an acknowledgement signal to the client system and waits for a confirmation signal from the client system confirming the receipt of the acknowledgement signal (steps 25 and 26). If confirmation is not received from the client system, the previously negotiated SA is used to secure traffic communication in step 30. On the other hand, if confirmation is received, the newly refreshed SA is used to secure traffic communication in step 27.

Figure 5 illustrates processes for updating SA at a client system according to an embodiment of the invention. In step 40, the client system determines whether there is new SA available for storage. If new SA is not available, then the client system uses the previously negotiated SA that is stored in the client system to secure traffic communication until the new SA is available. If a new SA is available, the new SA is stored in the client system in step 41. According to an embodiment, the new SA is

stored in hardware of the client system, preferably a network device. In step 42, the client system indicates that the new SA is ready for use by sending the "SA is ready for use" signal to the server system. In step 43, the client system waits for the acknowledgement signal from the server system. If the acknowledgement signal is not received, then the client system restores the previously negotiated SA and uses it to secure the traffic communication in step 52. If the acknowledgement is received, the client system sends the confirmation signal to the server client in step 44. In step 45, the new SA is used to secure the traffic communication.

According to one embodiment, the client system provides configuration options such that it can be managed with or without security. When a new client system is installed and does not have any OS present, the key exchange processes cannot be executed. The new client system is managed without security through configuration options by using some non-volatile storage such as an EEPROM or a register. By setting appropriate bits on the non-volatile storage, securing traffic is controlled. In another embodiment, a server system fails and becomes non-operational while the client system becomes non-operational. As a result, SAs on the server system are lost and no longer exist on the server system. In this case, the server system implements a persistent store for storing SAs that are in use with a plurality of client systems. The previously negotiated SAs are then easily restored. The persistent store may be some non-volatile storage such as an EEPROM.

Figure 6 shows a table illustrating the relationship between a server system and a client system during different state transitions according to an embodiment. Each row represents a transition state for the client system and the server system, and describes

attributes of the transition state. The first column of the table represents the state of the client system, and the second column represents the state of the server system. The third column describes attributes of the transition states.

In the embodiment, the states the server system or the client system could be in are "OS up," "OS Hung," "Pre-boot," "OS suspend," "Cold boot," and "Any state." "OS up" represents a state when a system is fully operational, having IKE running on the system and an established security context. "OS Hung" represents a state when a system hangs after a successful boot, having a pre-established security context, but IKE being unavailable. "Pre-boot" represents a state when a system is reset, having a pre-established security context, but IKE being unavailable. "Cold-boot" represents a state when a system comes out cold, having no security context to rely upon. "OS suspend" represents a state when a system is temporarily suspended, e.g., to conserve power when not being used (the system comes back into OS up state via a wake up event). In this state, the system has a pre-established security context, but IKE is unavailable. "Any state" refers to any of the above mentioned states.

According to one embodiment, IPSec traffic is keyed by a total cost of ownership (TCO) port, wherein the policies that are set for securing the TCO port are as follows: SA lifetime = infinite (either in time or kilobytes), Protocol = UDP, IPSec protocol = ESP + AH, Destination port = 298h, other parameters = Wildcards. Row 2 indicates the case where the server system is "OS up" and the client system transitions to an "OS up" state. Since both systems are "OS up," they are fully operational with the IPSec stack on both systems. This allows for regular IPSec traffic keyed by the TCO port. When the client system transitions to an "OS up" state, a SA refresh is employed, and new SA

would be updated in the client system and used to secure the traffic communication if there is a successful completion of the SA refresh. This ensures that there are no sequence number synchronization issues that have to be addressed.

Row 3 indicates the case where the server system is "OS up" and the client system transitions to an "OS hung" state. Row 4 indicates the case where the server system is "OS up" and the client system transitions to a "Pre-boot" state. Row 5 indicates the case where the server system is "OS up" and the client system transitions to a "OS suspend" state. When the client system undergoes a transition from an "OS up" state to a "OS hung," "Pre-boot" or "OS suspend" state, the previously negotiated SA stored in the client system is inhibited from being updated until a successful execution of another set of key exchange processes between the server system and the client system. In this case, the previously negotiated SA is still operational because it is stored in the client system. According to an embodiment, the server system stops renegotiating new SA by not completing a SA refresh since IKE does not exist anymore, and the server system continues to use previously negotiated SA to secure traffic communication. In other embodiments, selective communication is permitted on an insecure port, which can be enabled based on lack of communication with the server.

Row 6 indicates the case where the server system is "OS up" and the client system is "Cold-boot." When the client system is in such state, the client system does not have any security information. For example, a new system is in "Cold-boot" when it is installed and does not have any OS present, and therefore, the key exchange part of the security protocol cannot be executed. According to one embodiment, the client system provides a configuration option such that it can be managed with or without

security. In this case, the client system sends traffic communication in the clear, preferably with restrictions on the data, to the server system. In order to make it easier on the server, the traffic communication sent in clear may be sent on a different UDP port.

Row 7 indicates the case where the server system is "OS hung" and the client system is "Any state." Under this condition the client system is unmanageable by the server system because the server system is non-operational. A fault tolerant system is implemented for this case, wherein the fault tolerant system switches the control from the "OS hung" sever to an "OS up" secondary server.

Row 8 indicates the case where the server system is "Cold-boot" and the client system is "OS Hung or Pre-boot." Since the server system is in "Cold-boot," the server system does not have any security information. According to one embodiment, the client system provides a configuration option such that it can be managed with or without security. In this case, the client system takes unilateral action and communicates on an insecure port. The client system sends traffic communication in the clear, preferably with restrictions on the data, to the server system.

Row 9 indicates the case where the server system is "Cold-boot" and the client system is "Cold-boot." Since both systems are in "Cold-boot," neither one has any security information. In this case, the traffic communication is in the clear on the insecure port until such time that a security context can be established.

While the description above refers to particular embodiments of the present invention, it will be understood that many modifications may be made without departing from the spirit thereof. The accompanying claims are intended to cover such

modifications as would fall within the true scope and spirit of the present invention. The presently disclosed embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims, rather than the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS

What is claimed is:

1. A computer network comprising:

a server system;

a client system, the server system and the client system executing processes to provide security mechanisms for securing traffic communication between the two systems, the processes including key exchange processes executed when the client system is in an operational state;

logic for detecting whether the client system is in operational state;

a storage device at the client system for storing the results of the key exchange processes;

logic for inhibiting the stored results of the key exchange from being updated until a successful execution of another set of key exchange processes between the server system and the client system;

logic for updating the stored results of the key exchange if the execution of the other set of key exchange processes is successful; and

logic for using results stored in the memory to secure the traffic.

2. The computer network of claim 1, wherein the logic for inhibiting the stored results of the key exchange from being updated is embodied in the client system.

3. The computer network of claim 1, wherein the logic for inhibiting the stored results of the key exchange from being updated is embodied in the server system.

4. The computer network of claim 1, wherein the state of the server system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

5. The computer network of claim 1, wherein the state of the client system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

6. The computer network of claim 1, further comprising logic for allowing the traffic communication between the server system and the client system to be sent without security.

7. The computer network of claim 1, wherein the client system is a network device.

8. The computer network of claim 1, wherein the storage device is at least one of an Ethernet device, a coprocessor connected to an Ethernet device, and non-volatile storage that is part of an Ethernet device.

9. The computer network of claim 1, wherein the logic for inhibiting the stored results of the key exchange from being updated includes:

logic for sending a signal acknowledging the successful execution of another set of key exchange processes; and

logic for sending a signal confirming receipt of the acknowledgement signal.

10. The computer network of claim 1, wherein the server system contains a storage device for storing the results of the key exchange processes.

11. The computer network of claim 1, further comprising logic for switching the server system to a second server system in the computer network if the server system becomes non-operational, the security mechanisms securing traffic communication between the second server system and the client system.

12. A computer readable medium for use in conjunction with a server system and a client system for providing security mechanisms for securing traffic communication between the server system and client system, the computer readable medium including computer readable instructions encoded thereon for:

detecting whether the client system is in operational state;

executing first key exchange processes between the server system and the client system when the client system enters the operational state;

storing the results of the first key exchange processes into the client system;

inhibiting the stored results from being updated until a successful execution of a second set of key exchange processes between the server system and the client system;

updating the stored results with the results obtained by the second set of key exchange processes if the execution of the second set of key exchange processes is successful; and

using either the stored results or the updated results to secure the traffic depending on whether the second set of key exchange processes is successful.

13. The computer readable medium of claim 12, wherein the state of the server system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

14. The computer readable medium of claim 12, wherein the state of the client system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

15. The computer readable medium of claim 12, further comprising computer readable instruction encoded thereon for allowing the traffic communication between the server system and the client system to be sent without security.

16. The computer readable medium of claim 12, wherein the results of the key exchange processes are stored into at least one of a network device, a coprocessor connected to a network device, and non-volatile storage that is part of a network device.

17. The computer readable medium of claim 12, wherein the instruction for inhibiting the stored results of the key exchange from being updated includes:

sending a signal acknowledging the successful execution of the second set of key exchange processes; and

sending a signal confirming receipt of the acknowledgement signal.

18. The computer readable medium of claim 12, further comprising computer readable instruction encoded thereon for storing the results of the key exchange processes into the server system.

19. The computer readable medium of claim12, further comprising computer readable instruction encoded thereon for switching the server system to a second server system in the computer network if the server system becomes non-operational, the security mechanisms securing traffic communication between the second server system and the client system.

20. A method of providing security mechanisms for securing traffic communication between a server system and a client system, the method comprising:

detecting whether the client system is in operational state;

executing first key exchange processes between the server system and the client system when the client system enters the operational state;

storing the results of the first key exchange processes into the client system;

inhibiting the stored results from being updated until a successful execution of a second set of key exchange processes between the server system and the client system;

updating the stored results with the results obtained from the second set of key exchange processes if the execution of the second set of key exchange processes is successful; and

using either the stored results or the updated results to secure the traffic depending on whether the second set of key exchange processes is successful.

21. The method of claim 20, wherein the state of the server system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

22. The method of claim 20, wherein the state of the client system includes at least one of "OS up," "OS Hung," "Pre-boot," "OS suspend" and "Cold boot."

23. The method of claim 20, further comprising the step of allowing the traffic communication between the server system and the client system to be sent without security.

24. The method of claim 20, wherein the results of the key exchange processes are stored into at least one of a network device, a coprocessor connected to a network device, and non-volatile storage that is part of a network device.

25. The method of claim 20, wherein the step of inhibiting the stored results of the key exchange from being updated includes:

sending a signal acknowledging the successful execution of the second set of key exchange processes; and

sending a signal confirming receipt of the acknowledgement signal.

26. The method of claim 20, further comprising the step of storing the results of the key exchange processes into the server system.

27. The method of claim 20, further comprising the step of switching the server system to a second server system in the computer network if the server system becomes non-operational, the security mechanisms securing traffic communication between the second server system and the client system.

ABSTRACT OF THE DISCLOSURE

A system and method of providing security mechanisms for securing traffic communicated from a server system to a client system independent of the state of the client system. The server system determines whether the client system has entered an operational state. When the client system is operational, key exchange processes are initiated between the two systems, the results of the key exchange processes being the parameters for use in securing traffic communication between the two systems. The results are stored in the client system. The results are inhibited from being updated in the client system until the server system is successful in completely executing another set of key exchange processes. The results are updated with the results obtained from successful execution of the other set of key exchange processes if the execution of the other set is successful. The traffic communication is thus secured based on whatever results are stored in the client system.

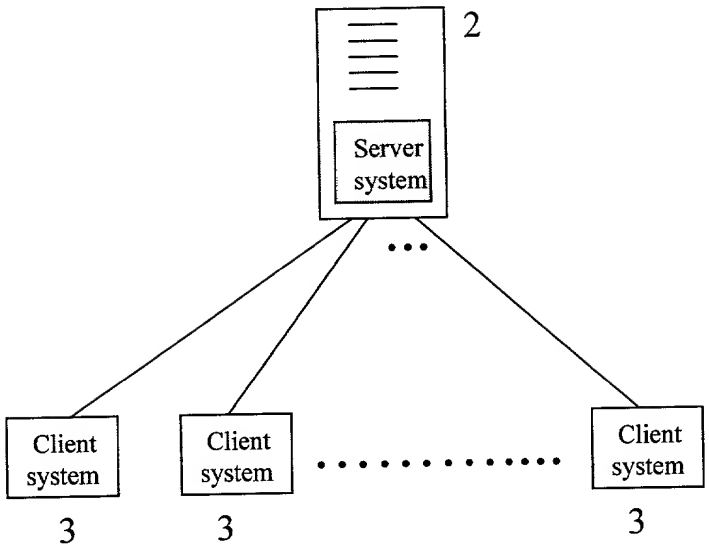

2
1
Server system
Client system
Client system
Client system
3
3
3

Fig. 1

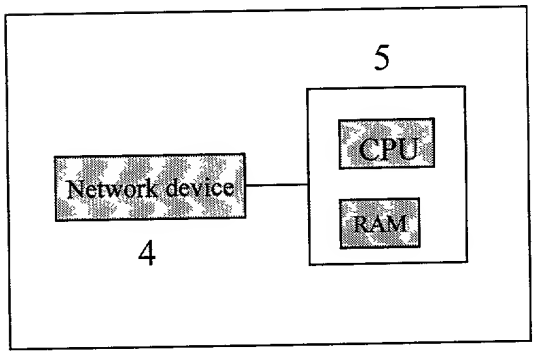

5
3
CPU
Network device
RAM
4

Fig. 2

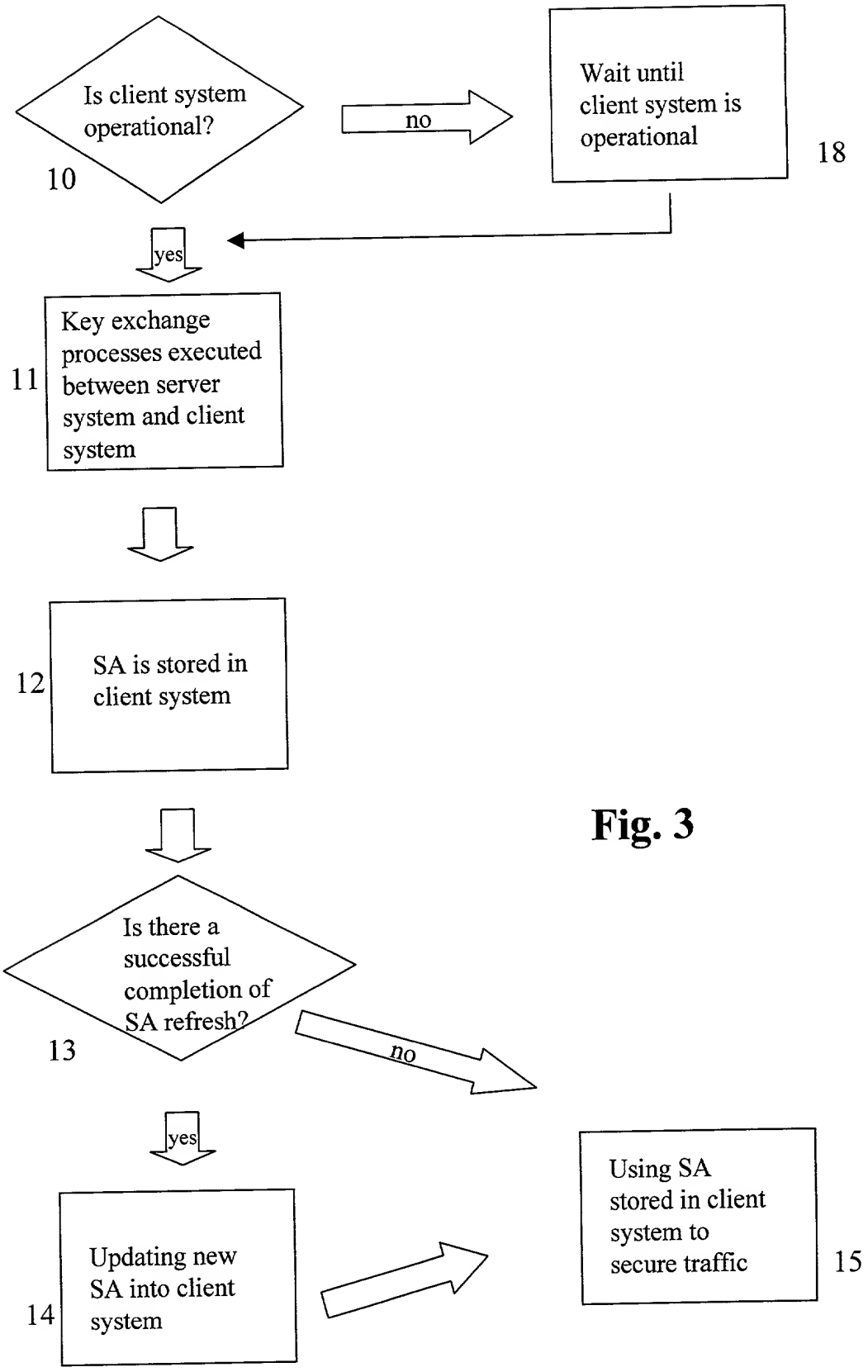

Is client system operational?
10
no
Wait until client system is operational
18
yes
Key exchange processes executed between server system and client system
11
SA is stored in client system
12
Is there a successful completion of SA refresh?
13
no
yes
Updating new SA into client system
14
Using SA stored in client system to secure traffic
15

Fig. 3

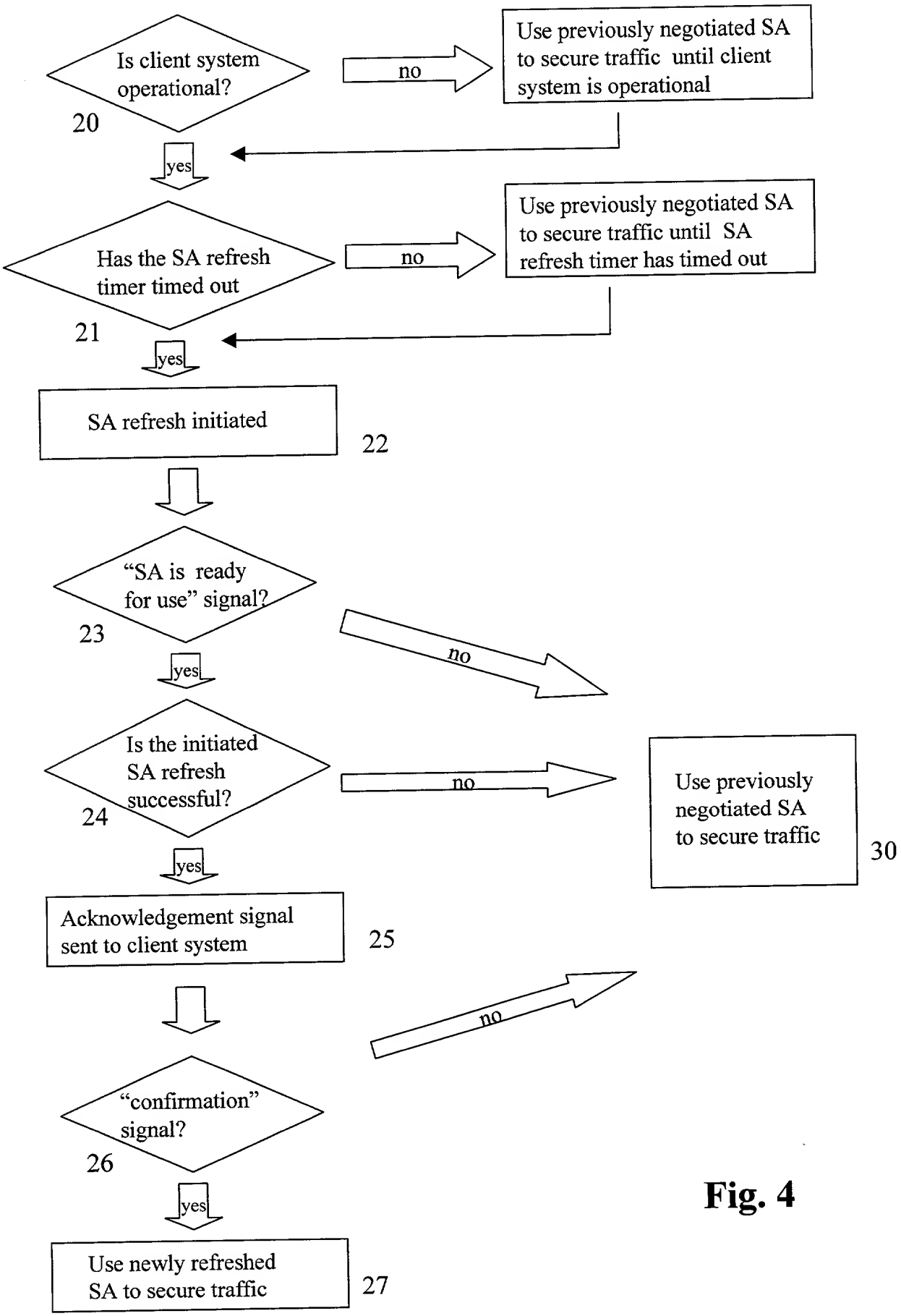

Is client system operational?
20
no
Use previously negotiated SA to secure traffic until client system is operational
yes
Has the SA refresh timer timed out
21
no
Use previously negotiated SA to secure traffic until SA refresh timer has timed out
yes
SA refresh initiated
22
"SA is ready for use" signal?
23
no
yes
Is the initiated SA refresh successful?
24
no
Use previously negotiated SA to secure traffic
30
yes
Acknowledgement signal sent to client system
25
no
"confirmation" signal?
26
yes
Use newly refreshed SA to secure traffic
27

Fig. 4

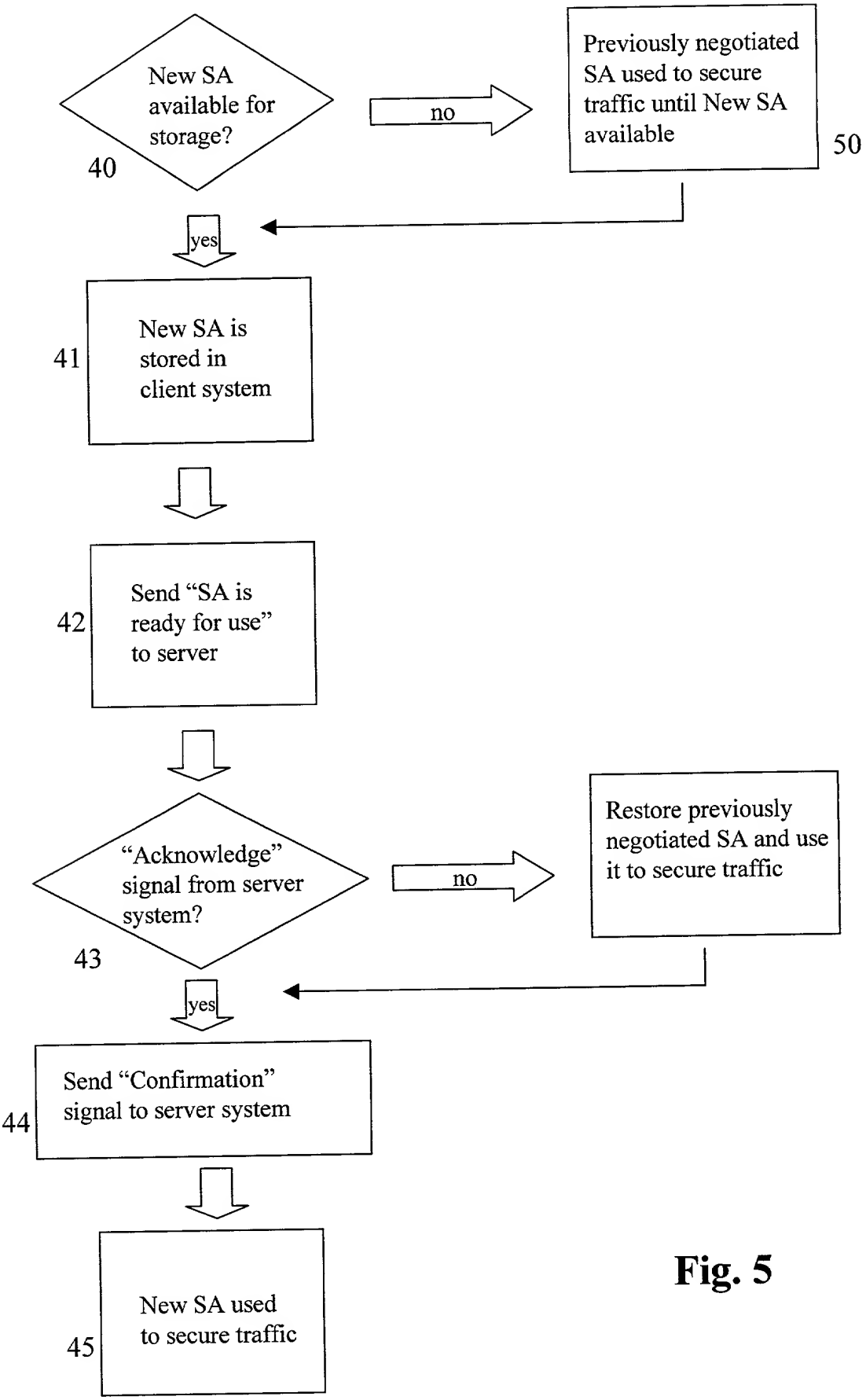

New SA available for storage?
40
no
Previously negotiated SA used to secure traffic until New SA available
50
yes
New SA is stored in client system
41
Send "SA is ready for use" to server
42
"Acknowledge" signal from server system?
43
no
Restore previously negotiated SA and use it to secure traffic
yes
Send "Confirmation" signal to server system
44
New SA used to secure traffic
45

Fig. 5

Fig. 6

State of Client System	State of Server System	Attributes of Transition States
OS up	OS up	IPSec stack on both client and server systems Newly negotiated SA Updated in client system if there is successful completion of SA refresh
OS hung	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
Pre-boot	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
OS suspend	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
Cold-boot	OS up	Client system does not have any security context Configuration option is provided for managing client system without security
Any state	OS hung	Client system is unmanageable by OS hung server system. Fault tolerant system is provided for switching control to secondary server system
OS hung / Pre-boot	Cold Boot	Server system does not have any security context Configuration option is provided for managing client system without security
Cold Boot	Cold Boot	Neither system has any security context Configuration option is provided for allowing traffic to be communicated in the clear

Attorney's Docket No.: P7775 / PMS264191

PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEM AND METHOD FOR PROVIDING SECURITY MECHANISMS FOR SECURING NETWORK COMMUNICATION

the specification of which

X is attached hereto.

___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number) Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint

Paul N. Kokulis, Reg. No. 16773; Raymond F. Lippitt, Reg. No. 17519; G. Lloyd Knight, Reg. No. 17698; Carl G. Love, Reg. No. 18781; Kevin E. Joyce, Reg. No. 20508; George M. Sirilla, Reg. No. 18221; Donald J. Bird, Reg. No. 25323; Peter W. Gowdey, Reg. No. 25872; Dale S. Lazar, Reg. No. 28872; Paul E. White, Jr., Reg. No. 32011; Glenn J. Perry, Reg. No. 28458; Kendrew H. Colton, Reg. No. 30368; G. Paul Edgell, Reg. No. 24238; Lynn E. Eccleston, Reg. No. 35861; Timothy J. Klima, Reg. No. 34852; David A. Jakopin, Reg. No. 32995; Mark G. Paulson, Reg. No. 30793; Stephen C. Glazier, Reg. No. 31361; Paul F. McQuade, Reg. No. 31542; Ruth N. Morduch, Reg. No. 31044; Richard H. Zaitlen, Reg. No. 27248; Roger R. Wise, Reg. No. 31204; Jay M. Finkelstein, Reg. No. 21082; Anita M. Kirkpatrick, Reg. No. 32617; Michael R. Dzwonczyk, Reg. No. 36787; W. Patrick Bengtsson, Reg. No. 32456; Jack S. Barufka, Reg. No. 37087; Paul G. Nagy, Reg. No. 37896; Steven W. Smyrski, Reg. No. 38312; Adam R. Hess, Reg. No. 41835; Eric S. Chen, Reg. No. 43542; Vivian S. Shin, Reg. No. 43919 my patent attorneys of PILLSBURY MADISON & SUTRO LLP, with offices located at 1100 New York Avenue, N.W., Washington, D.C. 20005-3918, telephone (202) 861-3000, and

Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Jeffrey S. Draeger, Reg. No. 41,000; Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256; and Alexander Ulysses Witkowski, Reg. No. P43,280; my patent agents, of INTEL CORPORATION; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to **Mr. Roger R. Wise, PILLSBURY MADISON & SUTRO LLP, 1100 New York Avenue, N.W., Washington, D.C. 20005-3918**, and direct telephone calls to **Mr. Roger R. Wise, (213) 488-7584.**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Anil Vasudevan

Inventor's Signature _____ Date _____

Residence Portland, OR (City, State) Citizenship Indian (Country)

Post Office Address 12849 NW Marshall Ct., Portland OR 97229

Full Name of Second/Joint Inventor Baiju V. Patel

Inventor's Signature _____ Date _____

Residence Portland, OR (City, State) Citizenship _____ (Country)

Post Office Address 10552 NW La Cassel Crest Lane, Portland OR 97229

Full Name of Third/Joint Inventor Marc Jalfon

Inventor's Signature _____ Date _____

Residence Zichron Yaakov, Israel (City, State) Citizenship Israel (Country)

Post Office Address Hasuka 18, Zichron Yaakov, 31015, Israel

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.